JOURNAL OF NUMBER THEORY 9, 160–174 (1977)

Ambiguous Divisor Classes in Function Fields*

MICHAEL ROSEN

Department of Mathematics, Brown University, Providence, Rhode Island 02912

Communicated by H. Zassenhaus

Received September 11, 1974

Let L/K be a Galois extension of algegraic function fields in one variable with Galois group G. Let J_K and J_L be the divisor classes of degree zero in K and L, respectively. A study is made of the kernel and cokernel of the natural map from J_K to $J_L{}^G$.

INTRODUCTION

Let K/k be an algebraic function field in one variable over a perfect constant field k. Let L/K be a finite Galois extension having the same constant field as K. Set $G = G(L/K)$ and J_L equal to the divisor classes of degree zero of L. There is a natural map $\alpha: J_K \to J_L{}^G$. We will investigate the kernel and cokernel of this map. The kernel is not hard to characterize. It is more difficult to analyze the cokernel. We shall give a cohomological description of it and exploit this in various ways.

When k is finite and G is cyclic, we obtain a formula for $| J_L{}^G |$. ($| S |$ denotes the number of elements in a set S.) This formula generalizes and sharpens a classical formula due to Schmidt and Moriya [9]. From this we are able to deduce an analog of a well-known result of Iwasawa [5] which holds in algebraic number fields.

Our methods enable us to give new proofs of some results of Madan (see [7, 8]). In particular we give a new proof of the theorem which states that when L/K is Galois and k is finite, then the class number of K divides the class number of L.

In addition to the class number it is interesting to investigate the rank of the class group. In this connection we prove a theorem (Theorem 14) which apparently has no analog in the case of number fields. Here, as elsewhere, the property which makes function fields more tractable than number fields is the simple nature of the units.

Finally, we consider the situation when k is algebraically closed. Among

* This Research was Partially supported by NSF Grant GP-29082.

ISSN 0022-314X

other things we are able to give a new proof and generalization of a theorem of F. Sullivan which deals with the points of order p on J_L, in the case where k is of characteristic p.

1. PRELIMINARIES[1]

To begin with, K will denote either a number field or a function field, and L/K a finite Galois extension with group G. The principal divisors, divisors, divisor classes, and units of K will be denoted by P_K, D_K, C_K, and U_K. Similarly for L. Let $P_1, P_2, \ldots, P_t$ be the primes of K which are ramified in L and $e_1, e_2, \ldots, e_t$, the respective ramification indices.

THEOREM 1. *The following sequences are exact.*

(A) $(0) \to H^1(G, U_L) \to {D_L}^G/P_K \to {C_L}^G \to H^1(G, P_L) \to (0)$.

(B) $(0) \to C_K \to {D_L}^G/P_K \to \sum Z/e_iZ \to (0)$.

Proof. From $(0) \to U_L \to L^* \to P_L \to (0)$ and Hilbert's Theorem 90 we deduce that ${P_L}^G/P_K \approx H^1(G, U_L)$. From $(0) \to P_L \to D_L \to C_L \to (0)$ and $H^2(G, D_L) = 0$ we deduce

$$(0) \to {P_L}^G \to {D_L}^G \to {C_L}^G \to H^1(G, P_L) \to (0)$$

is exact. Dividing the first two terms by P_K shows sequence (A) is exact.

Since $C_K = D_K/P_K$, sequence (B) will be shown to be exact if we can show ${D_L}^G/D_K \approx \sum Z/e_iZ$. Let P be a prime of K and $P = (\mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_g)^e = \Phi(P)^e$ be the prime decomposition of P in L. Then it is easy to see that the divisors $\{\Phi(P) \mid P \text{ a prime of } K\}$ constitute a free set of generators for ${D_L}^G$. The result is now immediate.

THEOREM 2. (A) *If* $H^2(G, U_L) = 0$, *then* $H^1(G, P_L) = 0$.

(B) *If* G *is cyclic,* $H^1(G, P_L) \approx W/N_{L/K}U_L$ *where* $W = U_L \cap N_{L/K}L^*$.

(C) *If* K *is a global field and at most one prime ramifies, then* $H^1(G, P_L) \approx H^2(G, U_L)$.

Proof. From $(0) \to U_L \to L^* \to P_L \to (0)$ and Hilbert's Theorem 90 we deduce $(0) \to H^1(G, P_L) \to H^2(G, U_L) \to^{\beta} H^2(G, L^*)$ is exact.

Part (A) follows immediately. If G is cyclic and M any G module, then $H^2(G, M)$ is isomorphic to the fixed elements of M modulo the norms. Thus β transforms into the natural map from $U_K/N_{L/K}U_L$ to $K^*/N_{L/K}L^*$. This proves part (B).

[1] A portion of the cohomological calculations given here are contained in unpublished course notes of Iwasawa [6].

To prove part (C) we need class field theory. Let P be a prime of K and $\mathfrak{P}$ a fixed prime of L lying above P. Let $L_{\mathfrak{P}}$ and K_P be the completions of L and K at $\mathfrak{P}$ and P, respectively. Let $G_{\mathfrak{P}} \subseteq G$ be the decomposition group of $\mathfrak{P}$. Then $G_{\mathfrak{P}} \approx G(L_{\mathfrak{P}}/K_P)$. Finally, let $n = [L : K]$ and $n(P) = [L_{\mathfrak{P}} : K_P]$. Local class field theory shows there is an isomorphism inv_P which maps $H^2(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*)$ injectively onto the group $(1/n(P))Z/Z$. Global class field theory shows there is an exact sequence

$$(0) \to H^2(G, L^*) \xrightarrow{i} \sum_{\mathfrak{P}|P} H^2(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*) \xrightarrow{\text{inv}} (1/n)\, Z/Z \to (0),$$

where i is obtained by combining the local restriction maps and inv is the sum of the local invariant maps. The sum of course is over all primes P of K.

If $\mathfrak{P} \mid P$ is unramified, then the composed map $H^2(G, U_L) \to H^2(G, L^*) \to H^2(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*)$ is the zero map. This is because $G_{\mathfrak{P}}$ is cyclic in this case and in the local unramified situation $L_{\mathfrak{P}}/K_P$ every unit is a norm. Thus if at most one prime ramifies, $i \circ \beta$ will have zero components except possibly at the one ramified prime, but since the sum of the local invariants is zero, the exception does not exist. Thus $i \circ \beta$ is the zero map. Since i is one to one, β is also the zero map. This proves part (C).

By combining Theorems 1 and 2 it is possible to give a unified proof for a number of scattered results on the behavior of class group extensions in number fields. Unfortunately this would lead too far away from our main subject matter, so we avoid this digression.

From now on we assume K is a function field with field of constants k and that L has k as constant field as well. We will assume further that K has a divisor of degree 1. This is always the case if k is either finite or algebraically closed.

Let $\deg_K$ denote the degree map on D_K, D_K^0 the divisors of degree zero, and $J_K = D_K^0/P_K$ the divisor classes of degree zero. Similarly for L. If D is a divisor of K, then $\deg_L D = [L : K] \deg_K D$. (See, for example, [3].)

Theorems 1 and 2 give information about the group of divisor classes. In function fields the divisor classes of degree zero are the center of interest and so we will have to supplement our discussion. We begin with the definition of two important invariants.

DEFINITION 1. Let $P_1, P_2, \ldots, P_t$ be the primes of K ramified in L. $\delta(L/K)$ is defined by

$$\delta(L/K) = (n, (n/e_1) \deg_K P_1, \ldots, (n/e_t) \deg_K P_t).$$

Here, as elsewhere, $n = [L : K]$.

DEFINITION 2. $\deg_L C_L^G$ is an ideal in Z. We define $d(L/K)$ to be the positive generator of this ideal.

Starting with Theorem 1, part (B) and the relation $\deg_L D = [L : K] \deg_K D$, we derive the following commutative diagram.

$$\begin{array}{ccccccccc} (0) & \to & C_K & \to & D_L{}^G/P_K & \to & \sum Z/e_iZ & \to & (0) \\ & & \downarrow{\scriptstyle \deg_K} & & \downarrow{\scriptstyle \deg_L} & & \downarrow{\scriptstyle \lambda} & & \\ (0) & \to & Z & \xrightarrow{n} & Z & \longrightarrow & Z/nZ & \to & (0). \end{array}$$

λ is the map induced on $\sum Z/e_iZ$ by $\deg_L$. It will play an important role in what follows.

PROPOSITION 1. *The image of λ is a cyclic of order $n\delta(L/K)^{-1}$. The kernel of λ has order $e_1e_2 \cdots e_t\delta(L/K)\, n^{-1}$.*

Proof. Let P be a prime of K and $P = (\mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_g)^e = \Phi(P)^e$ its prime decomposition in L. Then $\deg_L \Phi(P) = g \deg_L \mathfrak{P}_1 = gf \deg_K P$, where $f = f(\mathfrak{P}/P)$ is the local degree (see [3]). Now $efg = n$ so that $fg = n/e$ and so

$$\deg_L \Phi(P) = (n/e) \deg_K P.$$

Since the $\Phi(P)$ generate $D_L{}^G$, we deduce that $\delta(L/K)$ is a generator of the ideal $\deg_L(D_L{}^G) \subseteq Z$. (Note that we here use the existence in K of a divisor of degree 1.)

The size of the kernel and image of λ now follow easily from its definition.

Notice that if every ramified prime has degree 1, then $\delta(L/K) = n/[e_1, e_2, \ldots, e_t]$, where the brackets denote least common multiple. Also, if $n = \ell$ a prime, then $\delta(L/K) = \ell$ if ℓ divides the degree of every ramified prime and $\delta(L/K) = 1$ otherwise.

We are now in a position to modify Theorem 1 in a manner appropriate for function fields.

THEOREM 3. *If L/K is a finite Galois extension of function fields with the same constant field k, then the following sequences are exact.*

(A) $(0) \to H^1(G, k^*) \to D_L^{0G}/P_K \to J_L{}^G \to H^1(G, P_L) \to \Gamma \to (0)$, *where Γ is a cyclic group of order $\delta(L/K)\, d(L/K)^{-1}$.*

(B) $(0) \to J_K \to D_L^{0G}/P_K \to \ker \lambda \to (0)$.

Proof. The exactness of the first three terms in (A) follows from Theorem 1 and the obvious fact that a divisor class of finite order has degree zero.

Let α be the map from $D_L^{0G}/P_K \to J_L{}^G$. We will be done if we can show $(0) \to \operatorname{coker} \alpha \to H^1(G, P_L) \to \Gamma \to (0)$ is exact. This, however, follows

from the following commutative diagram, the snake lemma, and Theorem 1, part (A).

$$\begin{array}{ccccccccc} (0) & \to & D_L^{0G} & \to & D_L{}^G & \xrightarrow{\deg_L} & \delta(L/K)\,Z & \to & (0) \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow & & \downarrow & & \\ (0) & \to & J_L{}^G & \to & C_L{}^G & \xrightarrow{\deg_L} & d(L/K)\,Z & \to & (0). \end{array}$$

The number $\delta(L/K)$ is fairly easy to compute if L/K is given explicitly, but $d(L/K)$ is a more subtle invariant. The following theorem gives some information about it.

THEOREM 4. *If $\delta(L/K) = 1$, then $d(L/K) = 1$. Let $\bar{k}$ be the algebraic closure of k and suppose $H^2(G, \bar{k}^*) = 0$. If L/K is either unramified or if all the ramified primes have degree* 1, *then $d(L/K) = \delta(L/K)$.*

Proof. The first assertion is obvious since $d(L/K)$ divides $\delta(L/K)$.

If L/K is unramified $\delta(L/K) = n$ and if all ramified primes have degree 1, then $\delta(L/K) = n/[e_1, e_2, \ldots, e_t]$ as we have remarked previously.

Let $\bar{L}$ and $\bar{K}$ be derived from L and K by constant field extension to $\bar{k}$. The ramified primes $P_1, \ldots, P_t$ extend uniquely to $\bar{K}$ and their extensions are the primes of $\bar{K}$ ramified in $\bar{L}$. Moreover, the ramification indices $e_1, \ldots, e_t$ do not change. Thus $\delta(\bar{L}/\bar{K}) = \delta(L/K)$.

Since $H^2(G, \bar{k}^*) = (0)$ by hypothesis, we have $H^1(G, P_{\bar{L}}) = 0$ (see Theorem 2, part (A)). Applying Theorem 3, part (A), we conclude $\delta(\bar{L}/\bar{K}) = d(\bar{L}/\bar{K})$.

For a separable constant field extension the map $C_L \to C_{\bar{L}}$ is an injection. Moreover, the group G can be thought of as $G(\bar{L}/\bar{K})$ and we have $C_L{}^G \to C_{\bar{L}}{}^G$ is one to one. Since the degree of a divisor does not change under constant field extension, we conclude $d(\bar{L}/\bar{K})$ divides $d(L/K)$. But we have seen $\delta(L/K) = \delta(\bar{L}/\bar{K}) = d(\bar{L}/\bar{K})$. Thus $\delta(L/K)$ divides $d(L/K)$. In general it is true that $d(L/K)$ divides $\delta(L/K)$. Thus under the hypotheses of the theorem, $\delta(L/K) = d(L/K)$.

We isolate out the following special case for later use.

COROLLARY. *If L/K is cyclic and unramified, $d(L/K) = \delta(L/K) = n$.*

It is to be remarked that it is not always true that $\delta(L/K) = d(L/K)$. We will provide a counterexample later (Theorem 18).

The following theorem is a slight generalization of a result of Accola [1].

THEOREM 5. *Let M be the maximal abelian unramified extension of K in L. Then the kernel of the natural map from J_K to J_L is isomorphic to* $\mathrm{Hom}(G(M/K), k^*)$.

Proof. If L/K is unramified, then by Theorem 3 the kernel of $J_K \to J_L$ is $H^1(G, k^*) \approx \mathrm{Hom}(G, k^*) \approx \mathrm{Hom}(G/[G, G], k^*) = \mathrm{Hom}\,(G(M/K), k^*)$. Thus the theorem is true in this case.

In the general case, let E be the maximal solvable unramified extension of K in L. Then $\mathrm{Hom}(G(E/K), k^*) \approx \mathrm{Hom}(G(M/K, k^*)$, so we will be done if we can show $J_E \to J_L$ is one to one. To do this we will assume that a non-principal divisor D of E becomes principal in L and deduce from this the existence of a proper unramified abelian extension of E in L. This is a contradiction.

Suppose $D = (\alpha)$, where $\alpha \in L$. Let $\sigma \in G(L/E)$. Then $D = D^\sigma$ implies $\alpha^\sigma = \chi(\sigma)\alpha$, where $\chi(\sigma) \in k^*$. One sees easily that $\chi \in \mathrm{Hom}(G(L/E), k^*)$. Let m be the order of χ. We must have $m > 1$ since otherwise $\alpha \in E$ and D is principal in E. Now $\alpha^\sigma = \chi(\sigma)\alpha$ for all $\sigma \in G(L/E)$ shows $\alpha^m = a \in E$. Moreover, $(a) = mD$. It follows from Kummer theory that $E(\alpha)/E$ is a nontrivial abelian unramified extension of E in L. This cannot exist and so $J_E \to J_L$ is one to one as asserted.

COROLLARY. *$J_K \to J_L$ is one to one if either G has no abelian quotients or there is some prime of K totally ramified in L.*

2. APPLICATIONS WHERE k IS FINITE

Throughout this section we assume k is a finite field with q elements. As is well known, the group J_K is finite when the constant field of K is finite. We set $h_K = |\, J_K \,|$ and call h_K the class number of K.

THEOREM 6. *Suppose L/K is cyclic and unramified of degree n. Then the kernel and cokernel of $J_K \to J_L{}^G$ are both cyclic of order $(n, q - 1)$. In particular $|\, J_K \,| = |\, J_L{}^G \,|$.*

Proof. By the corollary to Theorem 4 we have $\delta(L/K) = d(L/K)$. Using this, the hypotheses, and Theorem 3, we have

$$(0) \to H^1(G, k^*) \to J_K \to J_L{}^G \to H^1(G, P_L) \to (0)$$

is exact.

Using part (C) of Theorem 2, we find $H^1(G, P_L) \approx H^2(G, k^*) \approx k^*/k^{*n}$. This latter group is cyclic of order $(n, q - 1)$. So is the group $H^1(G, k^*) = \mathrm{Hom}(G, k^*)$. This completes the proof.

THEOREM 7 (M. Madan [8]). *L/K a Galois extension. Then h_K divides h_L.*

Proof. A simple reduction shows it is sufficient to treat the case where G is simple. If G is nonabelian, then $h_K \mid h_L$ by the corollary to Theorem 5. If G

is simple and abelian, then it is cyclic of prime order. In this case any ramified prime is totally ramified. If there is some ramification, the result follows from the corollary to Theorem 5; if the extension is unramified, it follows from Theorem 6.

Our next goal will be to find a formula for $J_L{}^G$ in the case where G is cyclic. The final result will be a formula in which all the terms are reasonably easy to compute except the annoying invariant $d(L/K)$. In two special situations, however, this invariant will not appear. We afterwards consider in some detail the special case where G is cyclic of prime order.

DEFINITION 3. For a prime P of K let e be its ramification index in L and $d = \deg_K P$. We define

$$m(P) = (q^d - 1/(q^d - 1, e), q - 1).$$

Finally, we define $m(L/K) = (m(P_1),..., m(P_t))$, where $P_1,..., P_t$ are the primes of K ramified in L.

PROPOSITION 2. *Suppose G is cyclic and set $W = k^* \cap N_{L/K}L^*$. Then W is a cyclic group of order $m(L/K)$.*

Proof. By class field theory an element of K is a norm if and only if it is a norm everywhere locally.

Let P be a prime of K and $\mathfrak{P}$ a prime of L lying above P. In the local situation $L_{\mathfrak{P}}/K_P$, let $M_{\mathfrak{p}}$ be the maximal unramified intermediate extension. By the local structure theory there exist finite fields k_P and $k_{\mathfrak{p}}$ in K_P and $M_{\mathfrak{p}}$, respectively, and elements $T \in K_P$ and $U \in L_{\mathfrak{P}}$ such that

$$K_P = k_P((T)), \qquad M_{\mathfrak{p}} = k_{\mathfrak{p}}((T)), \qquad L_{\mathfrak{P}} = k_{\mathfrak{p}}((U)).$$

Moreover, $[k_P : k] = \deg_K P = d$, and $[L_{\mathfrak{P}} : M_{\mathfrak{p}}] = e$. It is now easy to see an element $\alpha \in k_{\mathfrak{p}} \subset M_{\mathfrak{p}}$ is a norm from $L_{\mathfrak{P}}$ if and only if it is an e'th power. Also, every element $a \in k_P \subseteq K_P$ is a norm from $M_{\mathfrak{p}}$. Using the transitivity of the norm, we conclude that $a \in k_P \subset K_P$ is a norm from $L_{\mathfrak{P}}$ if and only if it is an e'th power. If $a \in k$, it is thus a norm at P if and only if $a \in k^* \cap k_P^{*e}$. One easily sees that the order of this latter group is $m(P)$. W is the intersection of all these groups, so the order of W is $m(L/K)$ as asserted.

THEOREM 8. *Let L/K be cyclic of degree n over a finite constant field k with q elements. Then*

$$n(q - 1) \mid J_L{}^G \mid = h_K e_1 e_2 \cdots e_t m(L/K)\, d(L/K).$$

If all the ramified primes of K have degree 1, then

$$[e_1,..., e_t][(e_1, q - 1),..., (e_t, q - 1)] \mid J_L{}^G \mid = h_K e_1 e_2 \cdots e_t .$$

Proof. When k is finite, all the terms in sequence (A) of Theorem 3 are finite. Set the alternating product of these orders equal to one and solve for $| J_L{}^G |$. The result is

$$| J_L{}^G | = | D_L^{0G}/P_K | \, | H^1(G, P_L)| \, | H^1G, k^*)|^{-1} \, | \Gamma |^{-1}.$$

Using part (B) of Theorem 3 and Proposition 1, we have

$$n \, | D_L^{0G}/P_K | = h_K e_1 e_2 \cdots e_t \delta(L/K).$$

We know $| \Gamma | = \delta(L/K)\, d(L/K)^{-1}$.

Finally, from part (B) of Theorem 2 we see $H^1(G, P_L) \approx W/k^{*n}$. On the other hand, $H^1(G, k^*) \approx H^0(G, k^*) \approx k^*/k^{*n}$. Thus

$$| H^1(G, P_L)| \, | H^1(G, k^*)|^{-1} = | k^*/W |^{-1} = m(L/K)/q - 1.$$

Putting all this information together yields the first formula.

If all the ramified primes have degree 1, then $\delta(L/K) = d(L/K)$ by Theorem 4. Also, $\delta(L/K) = n[e_1, \ldots, e_t]^{-1}$ in this case. Finally, $m(P) = (q - 1/(q - 1, e), q - 1) = q - 1/(q - 1, e)$. Thus

$$m(L/K) = (q - 1)/[(q - 1, e_1), \ldots, (q - 1, e_t)].$$

Substituting this information into the first formula yields the second formula.

We point out once more that $\delta(L/K) = 1$ implies $d(L/K) = 1$ so that in this case the first formula in the theorem is especially simple.

We now specialize to the case where G is cyclic of prime order ℓ. As remarked earlier, $\delta(L/K) = \ell$ if $\ell \mid \deg_K P_i$ for $i = 1, \ldots, t$ and $\delta(L/K) = 1$ otherwise.

THEOREM 9. *Let L/K be a cyclic extension of prime degree ℓ.*

(A) *If $\delta(L/K) = 1$ and $q \not\equiv 1(\ell)$, then $| J_L{}^G | = h_K \ell^{t-1}$.*

(B) *If $\delta(L/K) = 1$ and $q \equiv 1(\ell)$, then $| J_L{}^G | = h_K \ell^{t-2}$.*

(C) *If $\delta(L/K) = \ell$, then $| J_L{}^G | = h_K \ell^{t-\epsilon}$, where $\epsilon = 1$ if $d(L/K) = 1$ and $\epsilon = 0$ if $d(L/K) = \ell$.*

Proof. We begin by calculating the invariant $m(L/K)$. From the definition of $m(P)$ we see immediately that if $q \not\equiv 1(\ell)$, then $m(P) = q - 1$ and consequently $m(L/K) = q - 1$.

If $q \equiv 1(\ell)$, then $m(P) = ((q^d - 1)/\ell), q - 1) = ((q - 1)/\ell)((q^d - 1)/(q - 1)), \ell) = ((q - 1)/\ell)(d, \ell)$. The last equality follows from $q^{d-1} + q^{d-2} + \cdots + 1 \equiv d(\ell)$ when $q \equiv 1(\ell)$. From this expression for $m(P)$ we deduce $m(L/K) = q - 1$ when $\delta(L/K) = \ell$ and $q - 1/\ell$ when $\delta(L/K) = 1$.

From these observations and the fact that $\delta(L/K) = 1$ implies $d(L/K) = 1$ we see that all three parts of the present theorem follow from the first formula of Theorem 8.

Remark. The calculation of $m(L/K)$ given in the proof of the theorem shows that when G is cyclic of prime degree ℓ, we have $H^1(G, P_L) \approx W/k^{*\ell}$ is trivial except when $\delta(L/K) = \ell$ and $q \equiv 1(\ell)$. In this later case it is cyclic of order ℓ. Using this one can prove Theorem 9 directly from Theorem 3.

Note, also, that if $\delta(L/K) = \ell$ and $q \not\equiv 1(\ell)$, then $H^1(G, P_L) = (0)$ and this implies $d(L/K) = \ell$. When $q \equiv 1(\ell)$, it is not clear if the situation $\delta(L/K) = \ell$ and $d(L/K) = 1$ is really possible.

The following theorem is an analog of Iwasawa's result in [5].

THEOREM 10. *Let L/K be a cyclic extension of prime degree ℓ. Then*

(A) *If $\delta(L/K) = 1$, $q \not\equiv 1(\ell)$, and $t = 1$, then $\ell \nmid h_K$ implies $\ell \nmid h_L$.*

(B) *If $\delta(L/K) = 1$, $q \equiv 1(\ell)$, and $t = 2$, then $\ell \nmid h_K$ implies $\ell \nmid h_L$.*

(C) *If $\delta(L/K) = \ell$, $d(L/K) = 1$, and $t = 1$, then $\ell \nmid h_K$ implies $\ell \nmid h_L$.*

In all other cases $\ell \mid h_L$.

Proof. If we assume $\ell \nmid h_K$, then by Theorem 9, $| J_L{}^G |$ is prime to ℓ in the three cases of the theorem and divisible by ℓ otherwise.

The result now follows since an ℓ-group acting on a nontrivial abelian ℓ-group has a nontrivial fixed point.

Remark. One can use Kummer theory to show that if $t = 1$ and $q \equiv 1(\ell)$, then $\delta(L/K) = \ell$. On the other hand, one can construct, using class field theory, examples where $t = 1$, $q \not\equiv 1(\ell)$, and $\delta(L/K) = 1$.

In the case of a noncyclic Galois group one cannot in general give precise results. Nevertheless, the following inequality is interesting.

THEOREM 11. *Suppose L/K is Galois with group G. Then*

$$n^2 \mid J_L{}^G \mid \geqslant h_K e_1 e_2 \cdots e_t d(L/K).$$

Proof. We omit the details. One uses Theorem 3, Proposition 1, together with the estimates $| \operatorname{Hom}(G, k^*)| \leqslant n$ and $| H^1(G, P_L)| \geqslant 1$.

Remark. This theorem is essentially due to Madan [7]. He proves $n^2 h_L \geqslant e_1 e_2 \cdots e_t h_K$ and also treats the non-Galois case.

When G is of special type, more precise results are possible. If $G = [G, G]$ and $H^2(G, k^*) = (0)$, then $| J_L{}^G | = h_K e_1 e_2 \cdots e_t \delta(L/K)$. These conditions hold if G is simple and the Schur multiplier of G is trivial. Examples of such groups can be found in [4].

We now turn our attention to the ℓ-rank of J_L, where ℓ is a prime dividing $n = |G|$. If A is an abelian group, $A(\ell)$ will denote the ℓ-primary component of A and ${}_\ell A$ the subgroup of elements of order dividing ℓ. The ℓ-rank of A is by definition the dimension of ${}_\ell A$ over $Z/\ell Z$. This number is denoted by $rk\,{}_\ell A$.

THEOREM 12. *Suppose L/K is cyclic of prime degree ℓ. Assume $\delta(L/K) = 1$ and $\ell \nmid h_K$. Then*

$$J_L(\ell)^G \approx \sum_1^r Z/\ell Z,$$

where $r = t - 2$ or $t - 1$ depending on whether $q \equiv 1(\ell)$ or not.

Proof. Using Theorem 9, we see that it is enough to show that with the given hypotheses $J_L(\ell)^G$ is an elementary abelian ℓ-group.

Let $N = e + \sigma + \sigma^2 + \cdots + \sigma^{\ell-1} \in Z[G]$ be the norm element (σ is a generator of G). If $\alpha \in J_L(\ell)^G$, then $N\alpha = \alpha^\ell$. On the other hand, $N\alpha$ is in the image of J_K and has order a power of ℓ. Since $\ell \nmid h_K$, we conclude raising to the ℓ'th power annihilates $J_L(\ell)^G$.

By making various other assumptions about G, $\delta(L/K)$, etc., it is possible to give other results of a similar nature. We content ourselves with the following theorem which is due to Madan, who also deals with the non-Galois case [7].

THEOREM 13. *Let L/K be Galois with Galois group G of order n. Let t_ℓ be the number of ramification incides divisible by ℓ. Then*

$$rk_\ell(J_L{}^G) \geqslant t_\ell - 1 - \mathrm{ord}_\ell\, n.$$

Proof. Using Theorem 3, part (A), we see

$$rk_l(D_L^{0G}/P_K) \leqslant rk_l(J_L{}^G) + rk_l(H^1(G, k^*)).$$

From Theorem 3, part (B) and Proposition 1, we see

$$t_l - 1 \leqslant rk_l(D_L^{0G}/P_K).$$

Finally, $H^1(G, k^*)$ has order dividing n so that its maximal possible ℓ-rank is $\mathrm{ord}_\ell\, n$.

In proving Theorem 13 we used the first three terms of the exact sequence of part (A) of Theorem 3. We will now use the last three terms of that sequence to prove a result of a different nature about $rk_\ell J_L{}^G$.

THEOREM 14. *Suppose L/K is Galois with group $G \approx \sum_1^s Z/\ell Z$, ℓ a prime. Suppose, further, that $q \equiv 1(\ell)$. Then*

$$rk_\ell(J_L{}^G) \geqslant (s(s+1)/2) - t - 1.$$

Proof. Let α denote the natural map from D_L^{0G} to $J_L{}^G$. In the proof of Theorem 3 we showed $(0) \to \operatorname{coker} \alpha \to H^1(G, P_L) \to \Gamma \to (0)$ is exact. Thus

$$rkH^1(G, P_L) \leqslant rk \operatorname{coker} \alpha + rk\Gamma \leqslant rkJ_L{}^G + 1. \tag{1}$$

(For ease of notation we have replaced rk_ℓ with rk.)

Now, $(0) \to H^1(G, P_L) \to H^2(G, k^*) \to^{\beta} H^2(G, L^*)$ is exact and by class field theory, $(0) \to H^2(G, L^*) \to^{i} \sum_P H^2(G_{\mathfrak{P}}, L_{\mathfrak{P}}{}^*)$ is exact. The notation was explained in the proof of Theorem 2, part (C). Let β_P be the composed map of β with the map from $H^2(G, L^*)$ to $H^2(G_{\mathfrak{P}}, L_{\mathfrak{P}}{}^*)$. If P is unramified, β_P is trivial since in the local unramified situation every unit is a norm. Thus

$$(0) \to H^1(G, P_L) \to H^2(G, k^*) \to \sum_{P_i} H^2(G_{\mathfrak{P}}, L_{\mathfrak{P}}{}^*)$$

is exact, where the sum is over the ramified primes. By class field theory the local cohomology groups are cyclic. Therefore

$$rkH^2(G, k^*) \leqslant rkH^1(G, P_L) + t. \tag{2}$$

Finally, we use a result of Yamazaki to compute $H^2(G, k^*)$. If $G = G_1 \times G_2$ and G acts trivially on A, then $H^2(G, A) \approx H^2(G_1, A) \oplus H^2(G_2, A) \oplus P(G_1, G_2; A)$, where the latter group is the group of pairings from G_1 and G_2 to A. See Theorem 2.1 and the remarks which follow in [11].

Using this and the hypothesis that $q \equiv 1(\ell)$, one deduces

$$H^2(G, k^*) \approx \sum_1^r Z/\ell Z, \qquad \text{where} \quad r = (s(s+1)/2). \tag{3}$$

From (2) and (3) we see

$$(s(s+1)/2) - t \leqslant rkH^1(G, P_L). \tag{4}$$

Combining (4) with (1) gives the desired result.

Remarks. The hypothesis $q \equiv 1(\ell)$ is crucial. If $q \not\equiv 1(\ell)$, then using the computation of $H^2(G, k^*)$ given in the theorem, one sees $H^2(G, k^*) = 0$ and so coker $\alpha = (0)$.

We give a construction of extensions L/K for which the theorem applies. Let K_i/K, $i = 1, \ldots, s$, be a cyclic extension of K of degree ℓ with $t_i \geqslant 1$ ramified primes. Assume the condition: P ramified in K_i implies P not ramified K_j for $i \neq j$. Then the fields are disjoint and $L = K_1 K_2 \cdots K_s$ is Galois over K with group isomorphic to $\sum_1^s Z/\ell Z$. There are $t = t_1 + t_2 + \cdots + t_s$ primes of K ramified in L. Moreover, there can be no constant

field extension. Assume $q \equiv 1(\ell)$ and $t_i \leqslant m$ for $i = 1, 2, \ldots, t$ and some integer m. Then by the theorem

$$rkJ_L^G \geqslant (s(s+1)/2) - sm - 1.$$

If we keep m fixed and let s increase, we get examples of fields with very large ℓ-rank.

We conclude this section with an application to Theorem 14 to towers of class fields.

For a function field K let $\tilde{K}$ be the maximal unramified elementary abelian ℓ-extension of K. By class field theory, $rk_\ell G(\tilde{K}/K) = rk_\ell J_K + 1$, where the $+1$ comes from the constant field extension of degree ℓ. Define a tower of fields by $K = K_0$, $\tilde{K} = K_1$, $\tilde{K}_1 = K_2$, etc.

THEOREM 15. *If $q \equiv 1(\ell)$ and $rk_\ell J_K \geqslant 3$, then $rk_\ell(J_{K_n}) \to \infty$ as $n \to \infty$.*

Proof. Let M_0 be the constant field extension of K_0 of degree ℓ. Then K_1/M_0 has no intermediate constant field exetnsions, is unramified, and $G(K_1/M_0)$ is an elementary abelian ℓ group of rank $\geqslant 3$. By Theorem 14, $rk_\ell J_{K_1}^G \geqslant (3 \cdot 4/2) - 1 = 5$. The theorem follows by repetition of the reasoning.

Closer attention to detail shows that the ℓ-ranks go to infinity at a tremendous rate; somewhat like 3^{2^n}.

3. Applications when k is Algebraically Closed

When k is algebraically closed, several simplifications take place. Since every prime has degree 1, the formula for $\delta(L/K)$ becomes $n[e_1, e_2, \ldots, e_t]^{-1}$. Moreover, J_K and J_L are divisible groups with a fairly well-known structure. Finally, $H^2(G, L^*) = (0)$ since by Tsen's theorem the Brauer group of a function field over an algebraically closed constant field is trivial. This implies $H^2(G, P_L) \approx H^2(G, k^*)$.

As an example of what can be proved when k is algebraically closed, we mention the following two theorems. The proofs use the above remarks and the by now standard arguments beginning with Theorem 3.

THEOREM 16. *If $H^2(G, k^*) = (0)$ and* char $k \nmid n$, *then*

$$(0) \to G/[G, G] \to D_L^{0G}/P_K \to J_L{}^G \to (0)$$

is exact.

COROLLARY. *Let L/K be a cyclic unramified extension. Then the natural map $\alpha: J_K \to J_L{}^G$ is onto.*

THEOREM 17. *Suppose L/K is unramified and $G \approx \sum_1^s Z/\ell Z$, where $\ell \neq$ char k is a prime. Then*

$$rk_\ell(J_L{}^G/\alpha(J_K)) \geqslant \frac{(s+1)(s-2)}{2}.$$

We shall now provide an example showing that $d(L/K) \neq \delta(L/K)$ in general.

Let E be an elliptic curve defined over k and let m be an integer not divisible by char k. Multiplication by m maps E onto E with kernel isomorphic to $Z/mZ \oplus Z/mZ$. The corresponding function field extension L/K is unramified and abelian with Galois group $G \approx Z/mZ \oplus Z/mZ$. Moreover, $J_L \approx J_K \approx E$ (see [2, p. 217]). The map α: $J_K \to J_L{}^G$ is onto since after identifying J_K and J_L with E, α corresponds to multiplication by m.

THEOREM 18. *For the extension L/K described above, $\delta(L/K) = m^2$ and $d(L/K) = m$.*

Proof. Since L/K is unramified of degree m^2, $\delta(L/K) = m^2$.

Since $J_K \to J_L{}^G \to H^2(G, k^*) \to \Gamma \to (0)$ is exact and α is onto, we have $H^2(G, k^*) \approx \Gamma$. By Yamazaki's theorem, $H^2(G, k^*) \approx Z/mZ$. The result now follows because Γ has order $\delta(L/K)\, d(L/K)^{-1}$.

From now on we assume char $k = p \neq 0$. We wish to study $rk_p J_L$. (By the p-rank of an abelian group we mean the p-rank of its torsion subgroup.) If $rk_p J_L = 0$, we say that L is singular.

THEOREM 19. *Suppose G is a p-group. Then $J_L{}^G \approx J_K \oplus \ker \lambda$. If L/K is unramified, $J_L{}^G \approx J_K$. If L/K is ramified,*

$$rk_p J_L{}^G = rk_p J_K + t - 1.$$

Proof. Since char $k = p$, k^* is uniquely p-divisible. It follows that both $H^1(G, k^*)$ and $H^2(G, k^*)$ are trivial. Thus

$$D_L^{0G}/P_K \approx J_L{}^G.$$

Since J_K is a divisible group, the sequence $(0) \to J_K \to D_L^{0G}/P_K \to \ker \lambda \to (0)$ splits. This proves the first assertion of the theorem.

By Proposition 1 the sequence $(0) \to \ker \lambda \to \sum_1^t Z/e_i Z \to^{\lambda} Z/nZ$ is exact and $|\operatorname{im} \lambda| = n\delta(L/K)^{-1}$. In the present case $\delta(L/K) = n[e_1, e_2, \ldots, e_t]^{-1}$. Therefore $\operatorname{im} \lambda$ is cyclic of order $[e_1, e_2, \ldots, e_t]$. Using the elementary divisors theorem and the fact that each e_i is a power of p, one can now show $rk_p \ker \lambda = t - 1$. (We omit the details). The second assertion of the theorem follows.

COROLLARY. *L is singular if and only if K is singular and at most one prime of K ramifies in L.*

We conclude with a generalization of a theorem of Sullivan [10].

THEOREM 20. *Suppose G is cyclic of degree p and that K is singular. Then* $rk_P J_L = (p-1)(t-1)$.

Proof. By Theorem 19, $J_L{}^G \approx J_K \oplus \ker \lambda$. Taking p-primary components and using the assumption that K is singular, we find $J_L(p)^G \approx \ker \lambda$ and so $rk_P J_L(p)^G = t-1$.

Since J_L is divisible, so is $J_L(p)$.

The remainder of the proof follows Sullivan's argument.

Let $N = e + \sigma + \cdots + \sigma^{P-1} \in Z[G]$, where σ is a generator of G. Then N annihilates $J_L(p)$ since the norm of an element is in J_K and by hypothesis J_K contains no elements of p-power order. Thus $J_L(p)$ is a module over $Z[G]/NZ[G]$ which is isomorphic to $Z[\zeta_p]$, where ζ_p is a primitive p'th root of unity. In $Z[\zeta_p]$ we have $p = u(1-\zeta_p)^{p-1}$, where u is a unit.

Let $H_i \subseteq J_L(p)$ be the kernel of the endomorphism $(1-\sigma)^i$. We have $H_i \subseteq H_{i+1}$ for all i. The relation $p = u(1-\zeta_p)^{P-1}$ and the fact that $J_L(p)$ is divisible show that $1-\sigma$ is onto and H_{p-1} is the kernel of multiplication by p. Thus we seek $rk_P H_{p-1}$.

The following sequence is exact:

$$(0) \to H_i \to H_{i+1} \xrightarrow{(1-\sigma)^i} J_L(p)^G \to (0).$$

The only nonobvious fact here is that the map $(1-\sigma)^i$ is onto. Let $\beta \in J_L(p)^G$. There is a $\gamma \in J_L(p)$ such that $(1-\sigma)^i(\gamma) = \beta$. Applying $1-\sigma$ to both sides shows $\gamma \in H_{i+1}$.

From the exact sequence it follows that $|H_{i+1}|/|H_i| = p^{t-1}$. Thus $|H_{p-1}| = p^{(p-1)(t-1)}$ and this completes the proof.

REFERENCES

1. R. ACCOLA, Vanishing properties of theta functions for abelian coverings of Riemann surfaces, *in* "Advances in the Theory of Riemann Surfaces," Annals of Mathematics Studies, No. 66, Princeton Univ. Press, Princeton, N.J. 1971.
2. J. W. S. CASSELS, Diophantine equations with special reference to elliptic curves, *J. London Math. Soc.* **41** (1966), 193–291.
3. C. CHEVALLEY, "Algebraic Functions of One Variable," American Mathematical Society Mathematical Surveys, Vol. VI, New York, 1951.
4. R. L. GRIESS, Schur multipliers of the known finite simple groups, *Bull. Amer. Math. Soc.* **78** (1972), 68–71.
5. K. IWASAWA, A note on class numbers of algebraic number fields, *Abh. Math. Sem. Univ. Hamburg* **20** (1956), 257–258.

6. K. IWASAWA, Notes for a course at Princeton, 1971, unpublished.
7. M. MADAN, Class number and ramification in fields of algebraic functions, *Arch. Math.* **19** (1968), 121–124.
8. M. MADAN, On class numbers in fields of algebraic functions, *Arch. Math.* **21** (1970), 161–171.
9. M. MORIYA, Rein arithmetische-algebraische Aufbau der Klassenkörpertheorie über algebraischen Funktionenkörpern einer Unbestimmten mit endlichem Konstantenkörper, *Japan J. Math.* **14** (1937–38), 67–84.
10. F. SULLIVAN, Ph. D. Thesis, University of Wisconsin at Madison, 1973.
11. K. YAMAZAKI, On projective representations and ring extensions of finite groups, *J. Fac. Sci. Univ. Tokyo* **10** (1964), 147–195.